THE CLAIMS

1. (Previously Presented) A methodology framework for analyzing technology system including a plurality of components and for designing security into that system, the framework comprising:

a first system which identifies the security threats for the solution;

a second system having a security reference model comprising a plurality of interrelated and interdependent security subsystems, the security subsystems further comprising an audit subsystem, an integrity subsystem, and an information flow control subsystem, the second system to determine security properties and functions of the information technology system in terms of the security subsystems;

a third system which is coupled to the second system and which allocates security properties to the components of the information technology system based upon the selected functions which are derived from the nature and number of the security subsystems within the information technology system;

a fourth system which is coupled to the third system for allocating the security properties to the components of the information technology system and which identifies functional requirements for the components, in terms of the Common Criteria, in order to comply with the security properties of the component allocated by the third system; and

a fifth system which is coupled to the fourth system and which documents the requirements for the security components for the information technology system.

2. (Previously Presented) A framework for designing security into an information technology system including the elements of Claim 1 wherein the second system which identifies security properties of the information technology system includes a component which uses security subsystems for identifying security properties.

3. (Previously Presented) A framework for designing security into an information technology system including the elements of Claim 2 wherein the standard criteria for identifying security properties includes a system which maps functions of security subsystems to an ISO standard 15408, also known as Common Criteria.

4. (Previously Presented) A framework for designing security into an information technology system including the elements of Claim 1 wherein the framework further includes a system which documents the solution and the security assumptions using a solution design security methodology.

5. (Previously Presented) A framework for designing security into information technology system including the elements of Claim 4 wherein the framework further provides integrity assurance requirements using a standard set of criteria.

6. (Previously Presented) A framework for designing security into an information technology system including the elements of Claim 5 wherein the standard set of criteria are in accordance with ISO 15408.

7. (Previously Presented) A method of designing security for an information technology system which includes insecure components, the steps of the method comprising:

identifying the security threats to the system;

determining the security properties within a reference model comprising a plurality of interconnected and interdependent security subsystems that, inter alia, manage audits, integrity, and information flow control;

assigning functional details of the plurality of security subsystems to an infrastructure, a plurality of components, and a plurality of operations of the system;

enumerating security requirements for the infrastructure, components and operations;

developing integrity assurance requirements; and

creating at least one functional technology diagram to document security requirements for the system.

8. (Previously Presented) A method of designing a secure solution including the steps of Claim 7 wherein the method further includes the step of ranking the security threats to the overall system and considering the biggest threats to the security properties of the overall system in terms of the security subsystems.

9. (Previously Presented) A method of designing a secure system including the steps of Claim 8 wherein the step of ranking the security threats to the security properties of the overall system includes the step of doing less for security threats not considered substantial threats to the security properties of the overall system in terms of the security subsystems.

10. (Previously Presented) A method of designing a secure system including the steps of Claim 7 wherein the method further includes the step of documenting the system environment and security assumptions and using the environment and security assumptions in developing the security properties of the overall system.

11. (Previously Presented) A method of designing a secure system including the steps of Claim 7 wherein the method further includes the step of developing integrity assurance requirements for the system and using those integrity assurance requirements in the functional technology diagram(s) for the system.

12. (Previously Presented) A method of securing a solution including the steps of Claim 7 wherein the step of determining the security properties of the overall system includes the step of using standard criteria for evaluating the solution.

13. (Previously Presented) A method of securing a solution including the steps of Claim 12 wherein the step of determining the security properties of the overall system includes the step of using the Common Criteria of ISO Standard 15408.

14. (Previously Presented) A method of securing a system including the steps of Claim 7 wherein the step of enumerating security requirements for infrastructure, components and operations includes the step of using an industry standard security criteria.

15. (Previously Presented) A method of securing a system including the steps of Claim 14 wherein the step of using an industry standard security criteria includes the step of using Common Criteria which conforms to ISO Standard 15408.

16. (Previously Presented) A method of securing a system including the steps of Claim 7 wherein the step of enumerating security requirements for infrastructure, components and operations includes the step of identifying, enumerating and describing a number of security subsystems that in total represent the security function of the solution.